REMARKS

Claims 1-30 are pending in the application. In the Office Action mailed August 30, 2006, the Examiner rejected claims 1-30 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,449,719 to Baker *et al.* (the "Baker patent") in view of U.S. Patent No. 6,810,525 to Safadi *et al.* (the "Safadi patent").

The disclosed embodiments of the invention will now be discussed in comparison to the prior art. Of course, the discussion of the disclosed embodiments, and the discussion of the differences between the disclosed embodiments and the prior art subject matter, do not define the scope or interpretation of any of the claims. Instead, such discussed differences merely help the Examiner appreciate important claim distinctions discussed thereafter.

Discussion of the Disclosed Embodiment

Applicant discloses, in one embodiment, a method for allowing a user at a remote computer system to access a computer resource, such as an application. A token is generated remote from the computer system, such as at a server, and is then transmitted to the user's computer system, such as by means of a smart card storing the token. The token contains encrypted user information including credit, authorization, and authentication information. The computer resource may be independently usable on the user's computer system or may be a module allowing remote access to an application or other resource stored on a server. The computer resource is encrypted such that the user may access it only upon completion of authorization and verification steps discussed below.

A request is initiated to open the encrypted computer resource stored on the computer system, and execution of a remote application manager component on the computer system is also initiated. Under the control of the remote application manager component, the token is decrypted and a user of the computer system is authenticated using authentication information stored in the token. Whether the user is authorized to use the requested computer resource using authorization information stored in the token is then verified, as is whether the user has sufficient credit contained in the token to use the requested computer resource using credit information stored in the token. When the user is authenticated, authorized, and has sufficient credit, the requested computer resource is decrypted and opened. Use of the computer resource is then monitored to determine whether the user has sufficient credit to continue using

the computer resource. A notification is provided when the monitored usage of the opened computer resource has exceeded the credit.

The disclosed embodiment provides the distinct advantage that it is usable in both continuous- and broken-connection modes of operations. That is to say that, the token may be used to verify and authenticate in instances where an application executes on the user's computer system and where the user interacts with an application executing on a remote server

Discussion of the Cited References

The cited references have a completely different principle of operation than the disclosed embodiment. Both the Baker and Safadi patents store and process tokens at remote servers and allow the client computer to decrypt content without reference to the token. Baker and Safadi therefore are only capable of providing ongoing authorization in the continuous-connection mode of operation.

Baker teaches a method including "sending URI, token, and user information to the streaming server, ... approving or disapproving a valid or invalid, respectively, URI and token combination on a transaction server, ... [and] providing a continuously encrypted data stream to the client if a valid URI and token combination was found." Col. 2, ln. 63-col 2., ln. 20.

Baker therefore clearly controls access to content only on the server and requires contact with the server in order to determine whether contact is allowed. None of the steps executed by the remote application management component are performed in the system of Baker. Baker also teaches only sending a stream of data and therefore does not teach or suggest the disclosed embodiment, which enables control of a stand-alone application stored on a user computer.

Safadi teaches a system in which a token is sent to a subscriber by an access controller. The token is then sent to a server. Then, "if the subscriber's entitlement to receive the IPPU selection is verified, the server will further process the IPPU selection for further enabling the selected service/application for use by the viewer." Col. 2, lns. 13-19.

Safadi therefore also evaluates the token only at the server and provides no means for evaluating the token at the client computer system. Safadi fails to perform any of the steps executed by a remote application management component on the subscriber terminal.

Discussion of the Claims

With respect to claim 1, the cited references, whether alone or in combination fail to teach all of the elements of claim 1. In particular, they fail to show, in combination with the remaining elements of claim 1, "transmitting the token to the computer system; transmitting a computer resource to the computer system, the computer resource being encrypted; initiating a request to open the computer resource stored on the computer system; *initiating execution of a remote application manager component on the computer system; under control of the remote application manager component, for both broken-connection and continuous connection environments, decrypting at the computer system the token and authenticating a user of the computer system using authentication information stored in the token*; verifying whether the user is authorized to use the requested computer resource using authorization information stored in the token; verifying whether the user has sufficient credit contained in the token to use the requested computer resource using credit information stored in the token." (emphasis added). Baker and Safadi describe only server based systems for token evaluation and authenticating and do not perform the steps recited in the claim.

With respect to claim 3, the cited references, whether alone or in combination, fail teach all of the elements of claim 3. In particular, they fail to show, in combination with the remaining elements of claim 3, a method "wherein the token is stored on a smart card that the remote application module component accesses to retrieve and decrypt the token." The passage from Safadi cited in the Office Action , Col. 2, lns. 7-10, fails to mention a smart card.

With respect to claim 10, the cited references, whether alone or in combination, fail to teach all of the elements of claim 10. In particular, they fail to show, in combination with the remaining elements of claim 10, a method including "providing a notification when the monitored usage of the opened computer resource has exceeded the credit comprises displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted." Neither Baker nor Safadi deal with controlling the use of applications and further fail to teach controlling access to applications as recited in claim 10.

With respect to claim 11, the cited references, whether alone or in combination fail to teach all of the elements of the claim. In particular, they fail to show, in combination with the remaining elements of claim 11, "receiving from the server system, a token including

encrypted information generated from the user information provided by the client system; a remote application manager component; and at least one computer resource, each computer resource being encrypted and the particular computer resources received being determined from the authorization information contained in the provided user information; *under control of the remote application manager component on the client system, decrypting at the client system the token in response to a request to initiate execution of one of the computer resources ... [and] verifying whether the user has sufficient credit contained in the token to use the requested computer resource.*" (emphasis added). Baker and Safadi describe only server based token evaluation and authenticating and do not perform the steps recited in the claim.

With respect to claim 12, the cited references, whether alone or in combination fail to teach or suggest a method "wherein the token is stored on a smart card that the remote application module component accesses to retrieve and decrypt the token." Neither Baker nor Safadi make any mention of a smart card.

With respect to claim 18, the cited references, whether alone or in combination, fail to teach or suggest a method "wherein providing a notification when the monitored usage of the opened computer resource has exceeded the credit comprises displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted." Neither Baker nor Safadi deal with controlling the use of applications and further fail to teach controlling access to applications as recited in claim 18.

With respect to claim 19, the cited references, whether alone or in combination, fail to teach all of the limitations of the claim. In particular, the cited references fail to teach, in combination with the other limitations of claim 19, a method including the steps of "generating a token including encrypted information generated from the user information provided by the client system; sending the token to the client system; sending a remote application manager component to the client system; sending at least one computer resource to the client system, each computer resource that is sent being encrypted; ... *decrypting at the client system the token and authenticating a user of the client computer system; verifying at the client system whether the user is authorized to use the computer resource; [and] verifying at the client system whether the user has sufficient credit contained in the token to use the computer resource.*" (emphasis

added). Baker and Safadi describe only server based systems for token evaluation and authenticating and do not perform the steps recited in the claim.

With respect to claim 20, none of the cited references, whether alone or in combination, teach or suggest a method "wherein the token is stored on a smart card that the remote application module component accesses to retrieve and decrypt the token." Neither Baker nor Safadi teach or suggest use of a smart card.

With respect to claim 26, none of the cited references, whether alone or in combination, teach a method "wherein providing a notification when the monitored usage of the opened computer resource has exceeded the credit comprises displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted." Neither Baker nor Safadi deal with controlling the use of applications and further fail to teach controlling access to applications as recited in claim 20.

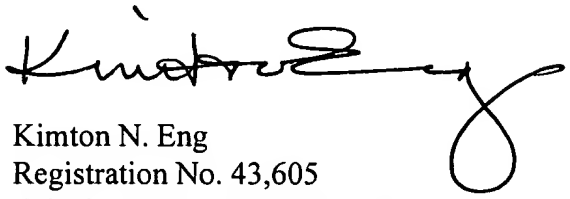
With respect to claim 27, the cited references fail to teach all of the limitations of the claim. In particular, the cited references, whether alone or in combination, fail to teach or suggest, in combination with the other limitations of the claim, a client system including "a remote application manager component being adapted to receive the encrypted user information contained in the token, *the remote application manager component operable responsive to a request to open a computer resource component to decrypt at the client system the encrypted user information, authenticate the user, determine whether the user is authorized to use the requested computer resource, and determine whether the user has sufficient credit to use the requested computer resource, the remote application manager component decrypting and opening the requested computer resource when the user is authenticated, authorized, and has sufficient credit*, and monitoring the usage of the opened computer resource and providing a notification when the monitored usage has exceeded the user's credit." Baker and Safadi describe only server based systems for token evaluation and authenticating and do not disclose a remote application manager component as recited in the claim.

Claims 2-10, 12-18, 20-26, and 28-30 are dependent on allowable independent claims 1, 11, 19, and 27, respectively, and are therefore allowable for at least the reasons discussed hereinabove.

All of the claims remaining in the application are now clearly allowable. Favorable consideration and a Notice of Allowance are earnestly solicited.

Respectfully submitted,

DORSEY & WHITNEY LLP



Kimton N. Eng
Registration No. 43,605
Telephone No. (206) 903-8718

KNE/MGP:ajs

Enclosures:
Postcard
Check
Fee Transmittal Sheet (+ copy)

DORSEY & WHITNEY LLP
1420 Fifth Avenue, Suite 3400
Seattle, Washington 98101-4010
(206) 903-8800 (telephone)
(206) 903-8820 (fax)

h:\ip\clients\micron technology\700\500767.01\500767.01 amend after final reject 1.116 2.doc